Steganography—the New Intelligence Threat

EWS 2004

Subject Area Intelligence

Murphy, S.D.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2004		**00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Steganography--the New Intelligence Threat	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Marine Corps War College,Marine Corps University,Marine Corps Combat Development Command,Quantico,VA,22134-5067**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**10**	

Thanks to new computer tools, digital files can easily be altered to embed hidden documents, pictures, or virtually anything that is digital in nature. This process is called steganography, or “the art of hidden information.”[1] Hiding information within electronic files is relatively benign unless the originator is exploiting the capability to transmit classified information, espionage products, or terrorist plans undetected across the Internet. The rapidly growing use of steganography in today’s technologically advanced world poses a serious threat to national security resulting in the need for the U.S. military to dedicate resources to combat this threat.

BACKGROUND

The earliest records of steganography date back to 5 B.C. when a Greek prisoner wanted to send a secret message to his son-in-law encouraging a revolt.[2] The prisoner shaved the head of a slave and tattooed a message on his scalp. When the slave's hair had grown long enough, he was dispatched to deliver the message. Hundreds of other types of steganography have been used over time, including invisible inks, wax tablets, and incredibly small photo reductions, used by Germans in World War II, called microdots. Any method of hiding or covering up information so as not to be detected by others can be considered a type of steganography.

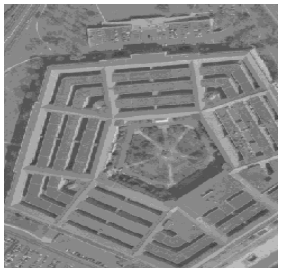
With the explosion of the digital era, steganography has experienced a rebirth. Now, more easily than ever, information can be hidden in digital files with minimal possibility of detection. Information can be embedded within text files, digital music and videos, and digital photographs by simply changing bits and bytes.

HOW IT WORKS

All digital files are made up of bits, which are just ones and zeros. A grouping of eight bits makes up a byte (Example of a byte: 0-1-0-1-0-1-0-1). The most common process of embedding files is based upon the idea that the last bit in each byte adds such a small amount of identity to the overall file that it could be modified without causing much visual or auditory change to the original file. New information could be stored in this last bit position of each byte until enough storage space is available to store a stolen classified document or a digital photograph taken by a spy. Considering that a PowerPoint file could easily be 10 megabytes in size, if the last bit of every byte was deleted to free up memory space for electronic bits of a hidden file, there would be 1.25 megabytes available ($1/8^{th}$ of the original file size) to hide data. This much space could store several Microsoft Word documents, multiple digital photographs, or even a short video clip.

If this process seems confusing, don't worry. Today's software does it all automatically. A Google search on the Internet for "steganography tools" nets 22,400 matches. Multiple software programs have the ability to take an original file, called a carrier file, and hide an embedded file within it. The carrier file is then transmitted without anyone ever knowing there is additional material embedded within it except for the file's intended recipient. The recipient, awaiting the hidden file, then uses steganography decryption tools to extract it from the carrier file. An example of an apparent innocent photograph embedded with an undetected photograph that could have intelligence value to terrorists is depicted below. Embedding the Pentagon photograph was accomplished using freely downloadable Steganography tools (Steghide, by Stefan Hetzl) on a home computer in just a few minutes. Notice undetectable changes to final embedded photo (carrier file):

Original Photo + Hidden Photo = Steganographic Photo


The process of embedding files lends itself to nearly every common file extension that most computer users are familiar with

(.txt, .html, .pdf, .wav, .jpg, .avi, .mpeg, .mp3, .tif, .gif, etc.). All of these file types can act as either the carrier or the embedded file. For instance, a digital photograph of troops at Baghdad International Airport could be embedded in Brittany Spears' latest music release in MP3 format. The wide range of steganography capabilities has been exploited by our adversaries.

ADVERSARY'S USE OF STEGANOGRAPHY

Exploiting steganography is more than hype; major threats to the U.S. are using this technology to endanger American lives. In a testimony on terrorism before a Senate panel in early 2001, Louis Freeh, the former FBI Director, briefed Congress, "Uncrackable encryption is allowing terrorists to communicate about their criminal intentions without fear of outside intrusion."[3] Freeh was referring to beliefs that Osama bin Laden and his al-Qaeda followers were hiding maps and photographs of targets, as well as terrorist plans, on the Internet through the use of steganography.[4] Embedded files are believed to be posted in sports chat rooms, pornographic bulletin boards, and other web sites for terrorists to download and unembed. In fact, the FBI discovered that three of the suspected hijackers in the 11 September hijackings rented hotel rooms in Hollywood, Florida, based upon the hotel's ability to provide 24-hour Internet access to their rooms.[5] Many experts argue that this requirement was to help the terrorist stay abreast of the developing bombing plan.

The stereotypical terrorist with a black mask and AK-47 is not fighting alone now. A new generation of computer literate America-haters have joined the ranks of terrorist cells and have expanded their capabilities. Terrorist groups that are well-armed, computer savvy, and determined to harm Americans pose a greater threat to U.S. security than ever before.

REAL OR UNJUSTIFIED THREAT

Despite the proven capability to use steganography to support terrorist actions, some analysts view the threat posed by this technology as unfounded and blown out of proportion. Niels Provos, a PhD candidate at the University of Michigan's Center for Information Technology Integration, developed a steganography detection program to search over two million photographs posted on eBay to see if any had embedded files.[6] His research identified no embedded files despite a USA Today article explaining how eBay could be an ideal place for terrorists to post embedded files. However, the use of steganography by terrorist groups cannot be discredited simply because eBay does not contain embedded files. Provos' research may prove that our adversaries are smart enough to find a less public site to store and transmit files.

Mr. Provos is not alone in believing that steganography is hardly a concern to the U.S. Robert Bagnall, a senior security analyst for Counterpane Internet Security Company, argues that our enemy has no need for steganography considering other

technological advancements that are widely available such as wireless networks, miniature mass media devices (MemorySticks, SmartCards, and so on).[7] He argues that new wireless technologies allow terrorists short duration access to digital information whenever and wherever needed without being observed or tracked. With this capability, Bagnall argues that the enemy does not need to waste time on embedding hidden files because they can be "in and out" with the necessary information faster than we can track them. Mr. Bagnall makes one false assumption. Just because our enemy can use wireless Internet capability does not mean that they won't use other methods to transmit data discretely. Having this variation in technologies between steganography and wireless networks makes detection of terrorists' plans even more difficult for U.S. intelligence analysts, computer technicians, and security personnel.

Despite the occasional disbeliever, steganography cannot be discredited as a threat, or at least, a potential threat. Most intelligence products are now produced and disseminated in electronic form. It is possible for these products to be captured, manipulated, and re-transmitted by anyone, at any time, to anyplace...undetected across the Internet. This, by its nature, is an incredible capability with wide application. The bottom line remains: Steganography IS a threat to U.S. national security.

WHAT CAN THE U.S. DO?

The United States prides itself on keeping up with technological change and remains a world leader in computer network defense. Therefore, we must allocate dollars, personnel, and expertise to find a solution and deter our enemy from further exploitation of this vulnerability. Failure to fight the problem now may lead to even greater threats in the future.

If the US is to make serious advancements in countering steganography, we must provide dedicated financial resources within the Department of Defense. Michael Vatis, a graduate student at Dartmouth's Institute for Security Technology Studies, pointed out that the US Commission on National Security recommended *doubling* the federal research and development budget by 2010 for counter-terrorism programs.[8] Money will drive private sector's interest in advancements as well as fund the government's ability to fight the problem. Once increased funding is addressed, the focus must turn to finding the right people for the job.

The organization best equipped to tackle potential steganography challenges is the National Security Agency (NSA) at Fort George Meade, Maryland. Although their personnel composition, budget, and specific technological capabilities are not advertised to the public, there is no secret about the focus of NSA in today's world. NSA's mission is to understand the

secret communications of our adversaries while protecting our own communications.[9] The cryptanalysis specialists at NSA could ideally fill the role as steganography detectors. Cryptanalysis is the art and science of solving ciphers or codes. Increasingly, it evolves into studying any type of hidden information in a variety of media.[10] NSA's employment of cryptanalysis specialists would be a starting point for building steganography expertise.

A renewed effort should be made to recruit many of the sharpest intelligence analysts and computer specialists to work for NSA. Personnel should come from military occupational specialties, civil service, and the private sector. Military organizations like the Navy's Fleet Information Warfare Center, Marine Corps Information Warfare Activity, Air Force Information Warfare Center, and the Army's 1st Information Operations Command all have potential talent pools to draw expertise. These technical experts, equipped with adequate funding and leading edge training, can diminish our vulnerability to steganography. Over time, our ability to detect, decrypt, and exploit hidden information will become our strength, not our weakness.

CONCLUSION

Undoubtedly, steganography can be used to support terrorist activities. Without a deliberate effort by the DoD to catch terrorists using steganography to pass dangerous intelligence to

their organizations, terrorists will continue exploiting this technology. Despite limited DoD resources, the military must dedicate manpower, develop expertise, and allocate money to better fight the technological battle against steganography and deter our enemy from using the Internet and other digital means to coordinate terrorist acts against us.

ENDNOTES

[1] The Oxford English Dictionary. Clarendon Press, Oxford, 1933.
[2] Newman, B. Secrets of German Espionage. London: Robert Hale Ltd, 1940.
[3] Jack Kelley, "Terror Groups Hide Behind Web Encryption", USA Today, 5 February 2001.
[4] Ibid.
[5] Tom Kellen, "Hiding in Plain View: Could Steganography be a Terrorist Tool?" SANS Institute, 2001.
[6] Niels Provos and Peter Honeyman, "Detecting Steganographic Material on the Internet," Center for Information Technology and Integration, University of Michigan, 2002.
[7] Robert Bagnall, "Reversing the Steganography Myth in Terrorist Operations", SANS Institute, 2002.
[8] Michael A. Vatis, "Combating Terrorism," Institute for Security Technology Studies at Dartmouth College, p13.
[9] "NSA Mission Statement", National Security Agency Homepage, http://www.nsa.gov/about_nsa/mission.html
[10] "Cryptanalysis", National Security Agency Website, http://www.nsa.gov/programs/employ/c.cfm